# GnuPGを用いた研究記録管理・公開システム構築

小林聡研究室

S023027 加藤未来

# 目的

- 研究データの捏造への対策として、記事の真正性と非改竄性を保持し、検証するシステム

＋

- 研究内容の進捗状況や内容を共有できる範囲を柔軟に指定可能するシステム

**研究記録公開制御システムの作成**

# 特徴

- SNS/Blog ベース
  …手軽な研究記録の作成・公開システム

- **記事毎の公開範囲の設定**
  …柔軟な公開範囲の指定を実現

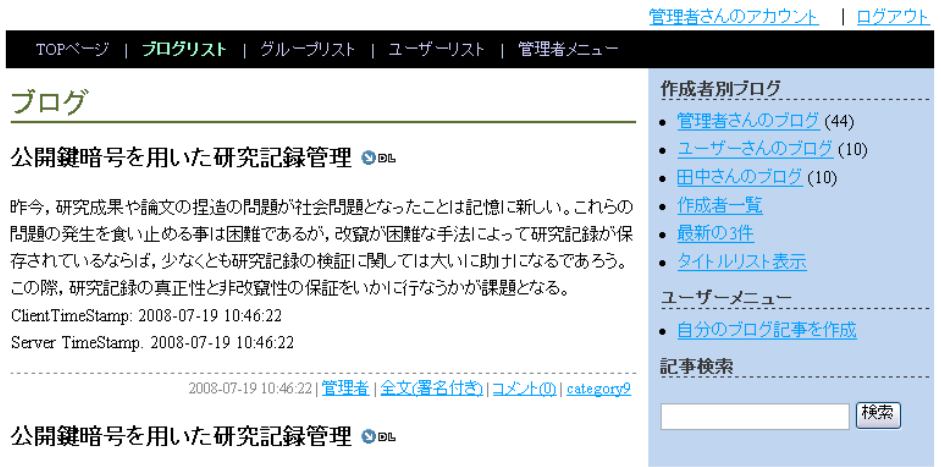
- **データの二重署名処理**
  …真正性と非改竄性の保証

# SNS/Blog ベース(1)

■ コンテンツ

- TOP ページ
- Blog リスト
- グループリスト
- ユーザリスト
- アカウントメニュー
- 管理者メニュー


TOP ページ




Blog リスト

表１　利用者別アクセス権限

| | 管理者 | ユーザ | ゲスト | 一般 |
|---|---|---|---|---|
| TOPページ | ○ | ○ | ○ | ○ |
| ブログリスト | ○ | ○ | ○ | ○ |
| グループリスト | ○ | ○ | ○ | |
| ユーザリスト | ○ | ○ | ○ | |
| アカウントメニュー | ○ | ○ | △ | |
| 管理者メニュー | ○ | | | |

△：自身の情報の閲覧のみ可能

- アカウントメニュー
  - ログイン利用者自身の情報の編集，削除が行える
- 管理者メニュー
  - システム全体の各データの編集，削除が行える

# グループについて

- グループ
  - 一人以上のユーザとゲストからなる利用者の集合
  - ユーザであれば誰でも作成可能
  - ユーザ全体で共有する
  - 管理は作成者及びシステム・ルートが行う
  - ルートとなるグループが存在する時、作成時に階層を持たせる事が可能（図1）

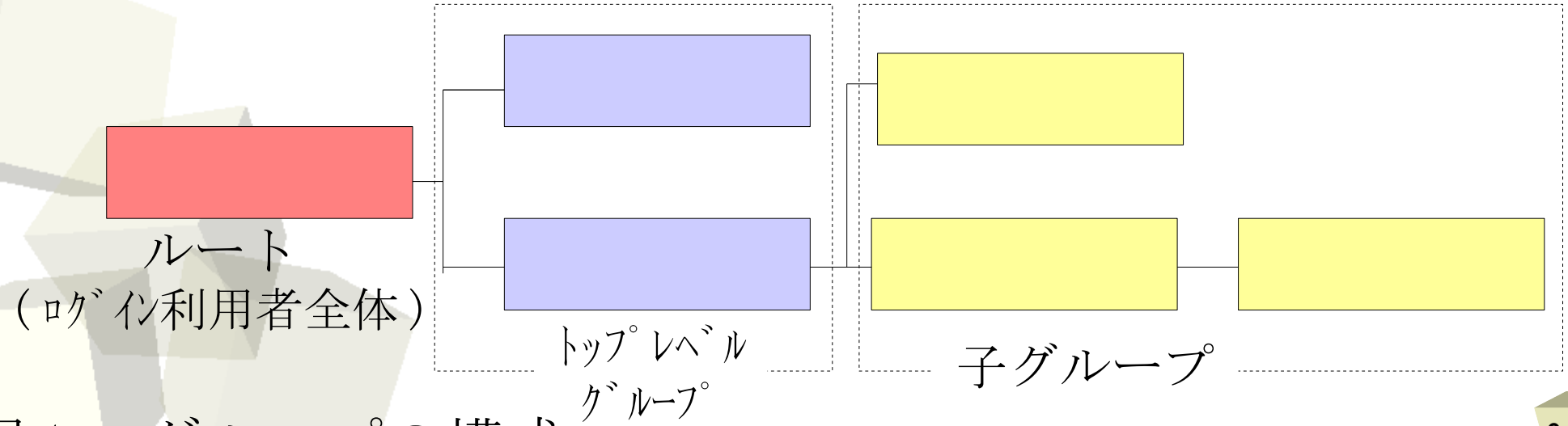



図１　グループの構成

# 記事毎の公開範囲の指定

- 大きく三段階で指定可能
  - ➔「自分のみ」,「グループ指定」,「全体公開」
  - 投稿後も公開範囲の変更が可能
- 「グループ指定」時
  - 複数のグループを指定可能
  - 指定グループの子グループも自動的に公開範囲に含める(図２)

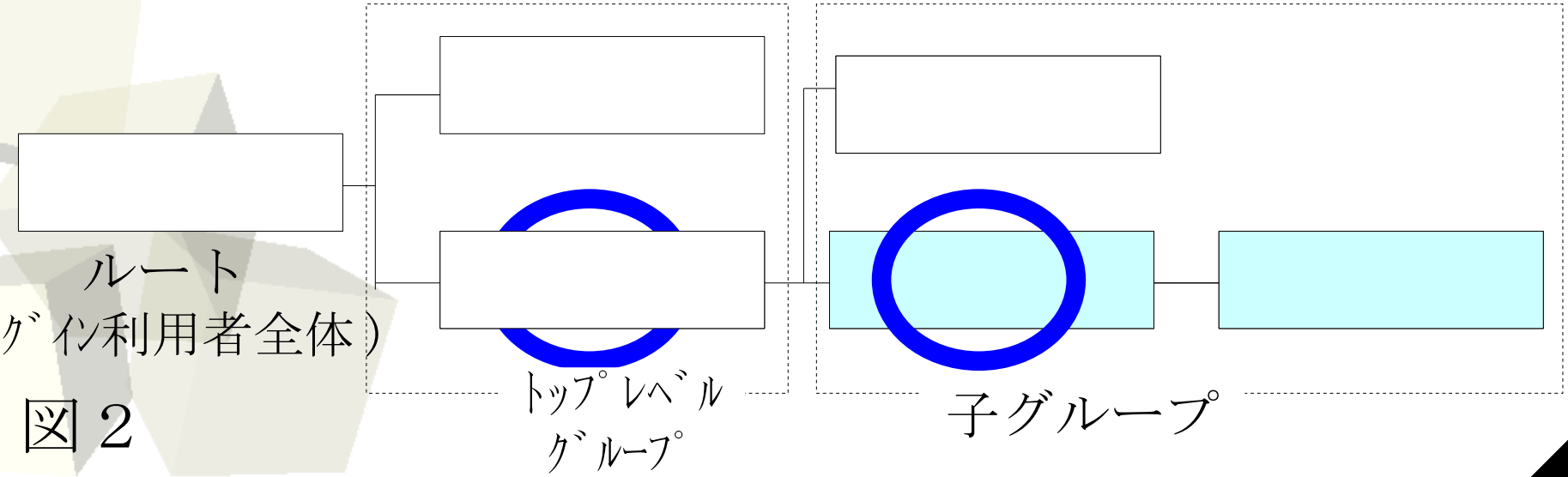



図２

# データの二重署名処理(1)

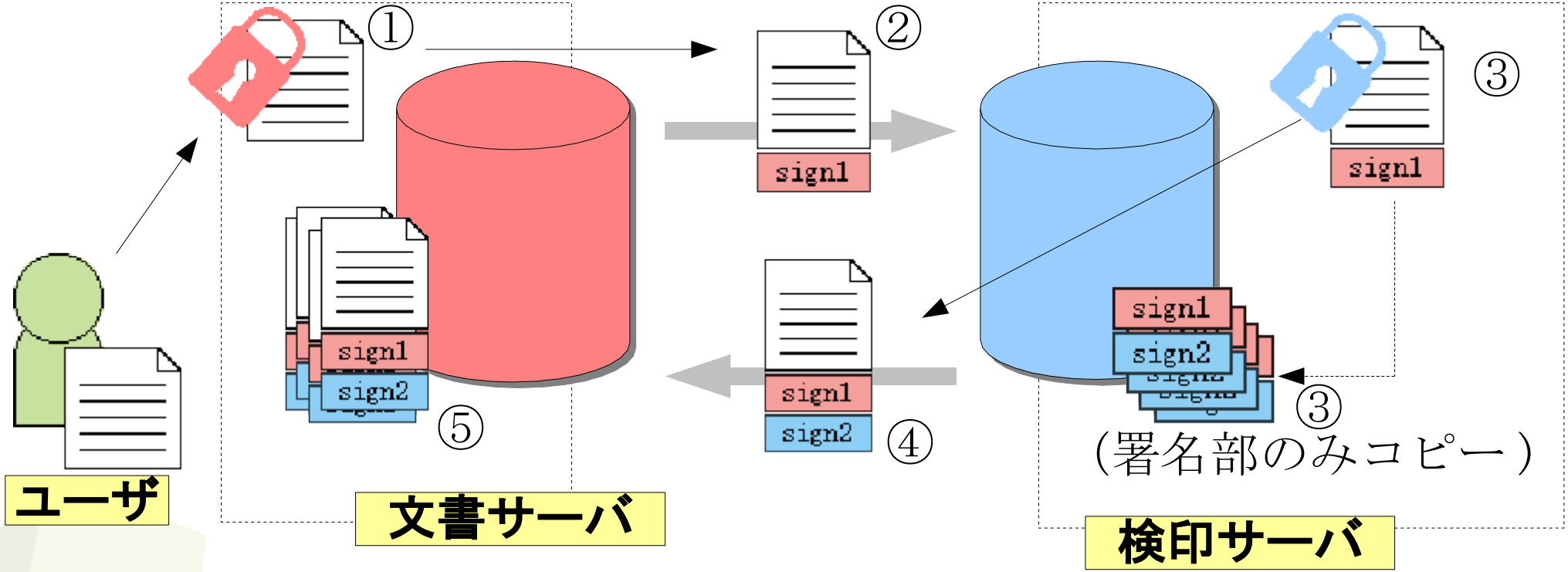
- 二重署名(検印モデル)とは:
  - 文書作成者自身の署名＋第三者による署名
    ⇒ 真正性と非改竄性を保証

電子データでも同様に、この署名作業を公開鍵暗号による電子署名で行うことで、真正性の保証をある程度実現可能。

『ライトワンス文書管理システム』，原田篤史ら
情報処理学会論文誌 Vol. 44, no. 8, pp. 2093-2105, 2003

# データの二重署名処理(2)

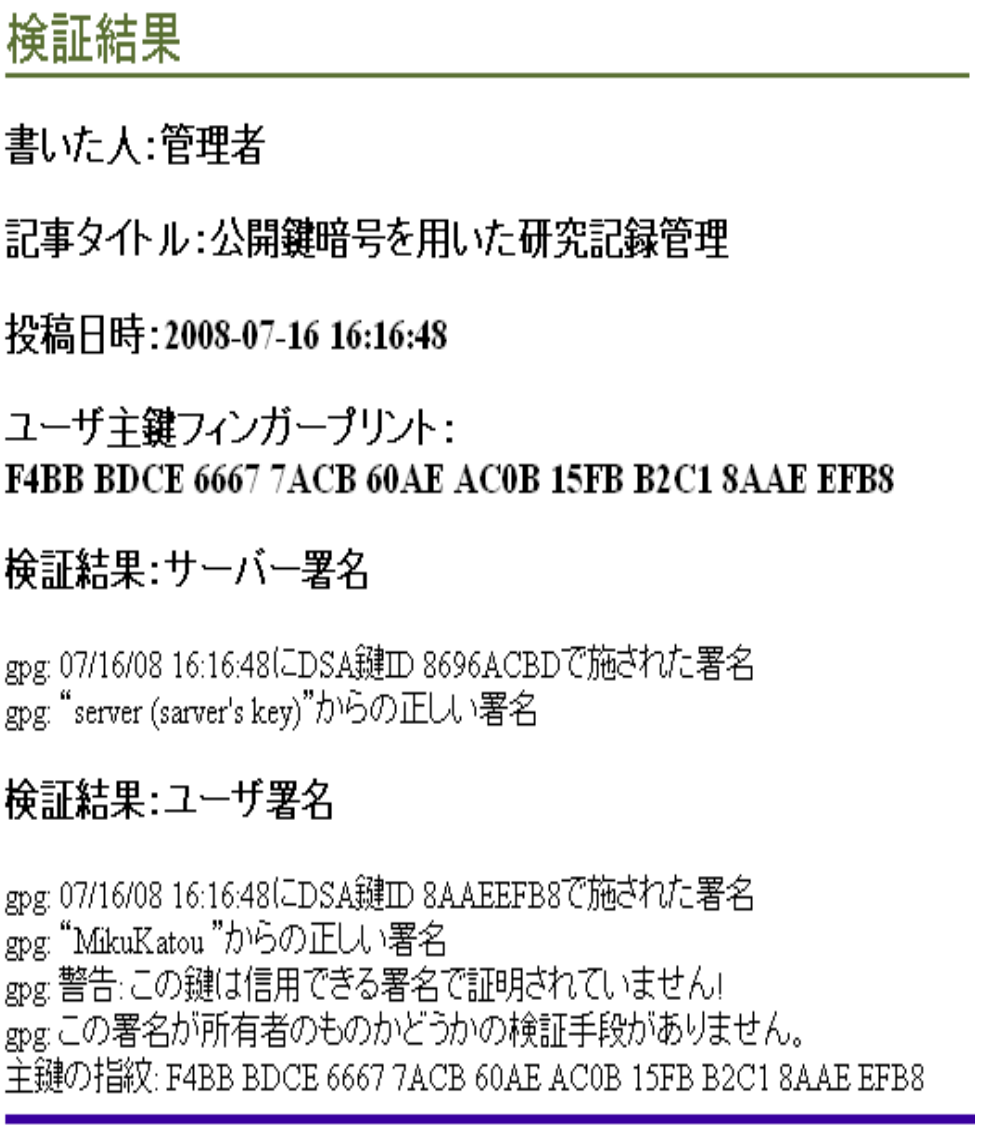
## 検印モデルの実装：データに対する二重署名




- 作成した文書にユーザ署名を行う
- 検印サーバへ転送
- 検印サーバで署名と署名部の保存
- 文書サーバに２重に署名済みのデータを送る
- 文書サーバにデータを保存

# その他の機能

- 各記事に対してデータファイルの添付機能
  - 添付されたデータファイルにも二重署名
- 記事や添付ファイルの検証機能
  - 投稿された記事のページから1クリックで検証が可能（図４）
  - 検証は『簡易検証』『通常検証』の２種
  - 手作業での検証も可能


検証結果

書いた人：管理者

記事タイトル：公開鍵暗号を用いた研究記録管理

投稿日時：2008-07-16 16:16:48

ユーザ主鍵フィンガープリント：
F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8

検証結果：サーバー署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8696ACBDで施された署名
gpg: “server (sarver's key)”からの正しい署名

検証結果：ユーザ署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8AAEEFB8で施された署名
gpg: “MikuKatou”からの正しい署名
gpg: 警告: この鍵は信用できる署名で証明されていません!
gpg: この署名が所有者のものかどうかの検証手段がありません。
主鍵の指紋: F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8

図４　検証画面

# 比較：記事毎の公開範囲の指定

## 類似システム：「Enzin」，「ACS」

### ■ 公開範囲

［共通］
- 自分のみ
- グループ（複数指定可）
- 全体公開

［相違点］
- ユーザ単位での指定（Enzin）
- パブリックリリース（ACS）
- グループの管理方法：
  - 個人（Enzin, ACS）
  - 利用者全体（本システム）
- グループに階層を作ることが可能（本システム）

### ■ 設定方法

| システム名 | 指定方法 | 変更 |
|---|---|---|
| Enzin | アイコンのドラッグ&ドロップによる指定 | 可 |
| ACS | チェックボックスによる指定 | 不可 |
| 本システム | テキストエリアへのグループ名の記入 | 可 |

「Enzin：情報の公開範囲を手軽に変更できるコミュニケーションツール」永田ら，情報処理学会論文誌， Vol. 48, no. 3, pp. 1134-1143, 2007
「ACS：多様な人間関係を表現可能なソーシャルネットワーキングシステム」高井ら，情報処理学会論文誌， Vol. 48, no. 7, pp. 2328-2339, 2007

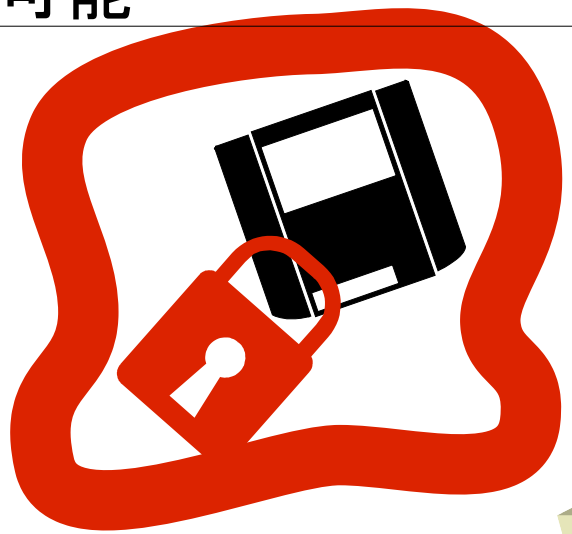
# 比較:真正性と非改竄性の保持

## 類似システム :「タイムスタンプサービス」

| | ﾀｲﾑｽﾀﾝﾌﾟｻｰﾋﾞｽ | 本システム |
|---|---|---|
| 非改竄性の保証の強度 | 高い | ﾀｲﾑｽﾀﾝﾌﾟｻｰﾋﾞｽに劣る |
| 検証効率 | 適宜問い合わせ | 記事ページより1クリック |
| 利用コスト | 一回10～2000円 | 導入までにｺｽﾄはかかるが，導入後は公開範囲の制御もでき，一般のBlogであるかのように手軽な利用が可能 |

- 非改竄性の高さをとるのであれば、タイムスタンプサービス
- ある程度の非改竄性を保持しつつ、頻繁に利用し、メモを残したいというものであれば本システム

という住み分けが可能と考えられる。



# 今後の課題

- セキュリティの問題
  - 非改竄性の証明の強度の向上
    - ➔ユーザの秘密鍵の保管方法
    - ➔公開鍵の正当性の確保
  - 署名時の文書サーバと検印サーバ間の通信時の情報漏洩への対策

- ユーザインタフェースの課題
  - 投稿･編集作業時のユーザインタフェースの改善
  - グループの管理の柔軟性向上
  - ユーザ認証の Delegate 機能の実装
  - 記事中での表や数式，化学式への対応
  - 漢字における異体字及び国字への対応

ご清聴ありがとうございました

# 実行画面各種：記事投稿

## ブログ記事の新規作成

| | |
|---|---|
| 筆者 | 管理者 |
| タイトル | 公開鍵暗号を用いた研究記録管理 |
| カテゴリ | category3 |
| 本文 | 昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。<br>この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。 |
| 記事公開範囲 | ○全体公開 ◉グループ公開 ○自分のみ<br>グループリスト<br>::GROUP2<br>::GROUP4:GROUP13<br>※閲覧を許可するグループ名を改行で区切り入力してください。<br>例)<br>::GROUP3<br>::GROUP10<br>… など |
| 添付ファイル | 参照…<br>備考・メモ |

プレビュー　投稿

## タイトル：公開鍵暗号を用いた研究記録管理

カテゴリ: **category3**

**≪本文≫**

昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。
この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。

**≪公開範囲≫**

::GROUP2:GROUP11
::GROUP2:GROUP11:GROUP15
::GROUP2
::GROUP4:GROUP13:GROUP17
::GROUP4:GROUP13

| | |
|---|---|
| 筆者 | 管理者 |
| タイトル | 公開鍵暗号を用いた研究記録管理 |
| カテゴリ | category3 |
| 本文 | 昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。<br>この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。 |
| 記事公開範囲 | ○全体公開 ◉グループ公開 ○自分のみ<br>グループリスト<br>::GROUP2<br>::GROUP4:GROUP13 |

新規作成画面・プレビュー画面

# 実行画面各種：記事閲覧

ブログ

## 公開鍵暗号を用いた研究記録管理

昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。
この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。
ClientTimeStamp: 2008-07-19 10:46:22
Server TimeStamp. 2008-07-19 10:46:22

2008-07-19 10:46:22 | 管理者 | 全文(署名付き) | コメント(0) | category9

## 公開鍵暗号を用いた研究記録管理

昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。
この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。
ClientTimeStamp: 2008-07-19 10:46:06
Server TimeStamp. 2008-07-19 10:46:07

2008-07-19 10:46:07 | 管理者 | 全文(署名付き) | コメント(0) | category3

## 公開鍵暗号を用いた研究記録管理

公開鍵暗号を用いた研究記録管理

---BEGIN PGP SIGNED MESSAGE-----
ash: SHA1

-----BEGIN PGP SIGNED MESSAGE-----
ash: SHA1

昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を
食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくと
も研究記録の検証に関しては大いに助けになるであろう。
この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。

lientTimeStamp: 2008-07-16 15:02:05
-----BEGIN PGP SIGNATURE-----
ersion: GnuPG v1.4.9 (MingW32)

YEARECAAYFAkh9jt0ACgkQFfuywYqu77h vwCg4TbT0j6VmA81itgNc918BVcj
7wAoNdd4g3dX7Wi/pKZpEcFoiZdGI/P
m2iZ
-----END PGP SIGNATURE-----

erver TimeStamp. 2008-07-16 15:02:05
---BEGIN PGP SIGNATURE-----
ersion: GnuPG v1.4.9 (MingW32)

YEARECAAYFAkh9jt0ACgkQNkcjG4aWrL3U1ACeITAQY/cnvgo1/oVYuhRN7h9
moAoIErpmkVJm9DRuTybs9EbndH217D
oqwK
-----END PGP SIGNATURE-----

公開範囲

::GROUP3:GRP12
::GROUP3:GRP12:GROUP16
::GROUP3

2008-07-16 15:02:05 | 管理者 | 簡易検証 | 通常検証 | コメント(0) | category3

一覧表示画面／詳細表示画面

# 実行画面各種:検証画面

## 検証結果

書いた人:管理者

記事タイトル:公開鍵暗号を用いた研究記録管理

投稿日時:2008-07-16 16:16:48

ユーザ主鍵フィンガープリント:
F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8

検証結果:サーバー署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8696ACBDで施された署名
gpg: “server (sarver's key)”からの 不正な 署名

検証結果:ユーザ署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8AAEEFB8で施された署名
gpg: “MikuKatou ”からの 不正な 署名

検証画面(データ改竄時)

添付ファイル： image01.gif [ダウンロード]
2重署名付きファイル("image01.gif.gpg") [ダウンロード]

テスト添付。
研究データの添付に利用できます。

[簡易検証] [通常検証]

公開範囲

::全体公開

2008-07-17 14:31:40 | 管理者 | 簡易検証 | 通常検証 | コメント(0) | category3

添付データ及び記事の検証画面

## 公開鍵のダウンロード

| ブログ名 | 書いている人 | 公開鍵ファイルの保存 | フィンガープリント |
|---|---|---|---|
| 管理者さんのブログ | 管理者 | ダウンロード | F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8 |
| ユーザーさんのブログ | ユーザ | ダウンロード | F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8 |
| 田中さんのブログ | 田中 | ダウンロード | F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8 |

| 署名サーバの公開鍵 | | |
|---|---|---|
| フィンガープリント | C55 3B84 FE90 709C DD47 C5FC DC00 4831 1294 5AC8 | ダウンロード |

公開鍵のダウンロード画面

# 実行画面各種：各コンテンツ画面

TOPページ | ブログリスト

## TOPページ

**システム・ルート（管理者）**

ログインID:admin, パスワード:pass

**ユーザ**

ログインID:user, パスワード:pass

**ゲスト**

ログインID:guest, パスワード:pass

**データファイルDL**

データDL⇒ 080610.lzh , 080715.lzh

・ログインをしなくても、ブログリストから全体公開されている記事の閲覧は可能です。

ユーザー専用ページ

ユーザー名:

パスワード:

ログイン

サブコンテンツ

- 公開鍵のダウンロード
- ブログ著者リスト

TOP ページ

管理者さんのアカウント | ログアウト

TOPページ | ブログリスト | グループリスト | ユーザーリスト | 管理者メニュー

## TOPページ

**システム・ルート（管理者）**

ログインID:admin, パスワード:pass

**ユーザ**

ログインID:user, パスワード:pass

**ゲスト**

ログインID:guest, パスワード:pass

**データファイルDL**

データDL⇒ 080610.lzh , 080715.lzh

・ログインをしなくても、ブログリストから全体公開されている記事の閲覧は可能です。

サブコンテンツ

- 公開鍵のダウンロード
- ブログ著者リスト

TOP ページ（ログイン後）

管理者さんのアカウント | ログアウト

TOPページ | ブログリスト | グループリスト | ユーザーリスト | 管理者メニュー

## グループリスト

ID順 | 階層順 | 名前順 検索

New 1 2 Old

| ID | グループ名 | 階層 | 登録者 | 登録者数 | 登録日 |
|---|---|---|---|---|---|
| 1 | :: | 0 | 管理者 | 15 | 2008/07/14 |
| 2 | ::GROUP2 | 1 | ゲスト | 3 | 2008/07/13 |
| 3 | ::GROUP3 | 1 | 佐藤 | 6 | 2008/07/12 |
| 4 | ::GROUP4 | 1 | 鈴木 | 1 | 2008/07/11 |
| 5 | ::GROUP5 | 1 | 高橋 | 2 | 2008/07/10 |
| 6 | ::GROUP6 | 1 | 管理者 | 1 | 2008/07/09 |
| 7 | ::GROUP7 | 1 | ユーザ | 2 | 2008/07/08 |
| 8 | ::GROUP8 | 1 | ゲスト | 2 | 2008/07/07 |
| 9 | ::GROUP9 | 1 | 佐藤 | 1 | 2008/07/06 |
| 10 | ::GROUP10 | 1 | 鈴木 | 3 | 2008/07/05 |

タイプ別

- ルートグループの表示

ユーザメニュー

グループの新規作成

ユーザーリスト画面

管理者さんのアカウント | ログアウト

TOPページ | ブログリスト | グループリスト | ユーザーリスト | 管理者メニュー

## ユーザーリスト

ID順 | 名前順 検索

1 2

| ID | 名前 | 登録日 |
|---|---|---|
| 1 | 管理者 | 2008/07/15 |
| 2 | ユーザ | 2008/07/15 |
| 3 | ゲスト | 2008/07/15 |
| 4 | 佐藤 | 2008/07/15 |
| 5 | 鈴木 | 2008/07/15 |
| 6 | 高橋 | 2008/07/15 |
| 7 | 田中 | 2008/07/15 |
| 8 | 渡辺 | 2008/07/15 |
| 9 | 伊藤 | 2008/07/15 |
| 10 | 山本 | 2008/07/15 |

- 全員
- ::GROUP10(3)
- ::GROUP2(3)
- ::GROUP2:GROUP11(3)
- ::GROUP2:GROUP11:GROUP15(1)
- ::GROUP3(6)
- ::GROUP3:GRP12(3)
- ::GROUP3:GRP12:GROUP16(1)
- ::GROUP4(1)
- ::GROUP4:GROUP13(1)
- ::GROUP4:GROUP13:GROUP17(0)
- ::GROUP5(2)
- ::GROUP5:GROUP14(1)
- ::GROUP6(1)
- ::GROUP7(2)
- ::GROUP8(2)
- ::GROUP9(1)
- ::(15)

グループリスト画面

# システムの利用者

- 利用者

  一般

  → 一部記事（Blogリスト）のみ閲覧可

**ログイン可能利用者**

→ ログイン ID/ パスワード所持

→ グループ所属可能

ゲスト

- 記事投稿不可

ユーザ

- 記事投稿可能

システム・ルート（管理者）

- システムの管理者

# 利用ツール

- 開発言語: Ruby（1.8.6）
- フレームワーク: Ruby on Rails（1.2.6）
- 公開鍵暗号ソフト: GnuPG（1.4.9）
- ウェブサーバ: Apache（2.0.6）
- SSLライブラリ: OpenSSL（0.9.8）

- DVCS（Data Validation and Certification Server Protocols）:
  - 
- TAP（Trusted Archive Protocol ）:
  - 